Signaling Prefix Origin Validation Results from an RPKI Origin Validating BGP Speaker to BGP Peers

draft-ietf-sidrops-validating-bgp-speaker
IETF 104, March 26 2019, Prague
Main idea

- In the domain of an IXP network, forward ROA validation results from a route server to its peers

Why?

- Lightweight method for peers to make use of RPKI for
  - using the validation results of the IXPs route server
  - monitoring, maintenance, troubleshooting
  - educational and research purposes
Signaling at an IXP

Signaling Prefix Origin Validation Results to Peers

draft-ietf-sidrops-validating-bgp-speaker-02
Current Implementation

Introduce a transitive four-octet AS Specific Extended Community, which signals:

1. ROA validity status of a prefix (Local Administrator field)
2. Signaling ASN (Global Administrator field)
Modes of operation

Allow for 3 modes of operation for validating BGP speaker:

1. **Tag prefixes** with their ROA validity status, and advertise them.
2. **Drop prefixes with ROA status "Invalid"**
   Tag the remaining "Unknown" and "Valid" routes, and advertise them.
3. **Drop prefixes with ROA status "Invalid" and "Unknown"**
   Tag the remaining "Valid" routes, and advertise them.
Rough Timeline

- 2015-12: First version of draft-kklf-sidr-route-server-rpki-light
- 2017-04: Added modes of operation
- 2018-01: Swapped RFC8097 community to EBGP Prefix Origin Validation Extended Community

Failed to hitchhike with draft-ietf-sidr-origin-validation-signaling now RFC8097
...Meanwhile

- Discussions on the mailing list, suggestions have been included
- RPKI adoption continues, e.g. dropping RPKI invalids at IXP route servers
- Demand for tagging of RPKI validation states with BGP communities persist

Continuing...

- With people asking for this draft, we would like to finalize/finish the draft
- Any input / idea / discussion is welcome